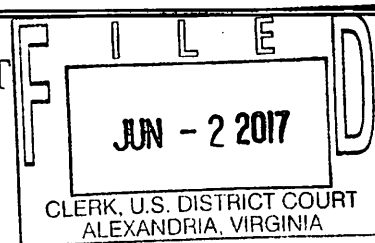


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

Apple iPhone model A1778, serial number
DNPSDABEHG7W, and an Apple iPad Model A1674,
serial number DMPS66Q8GXQ4, CURRENTLY
LOCATED AT 44965 Aviation Drive, Suite 112, Dulles, VA

Case No. 1:17-SW-303

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:
See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:


<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2252(a)(2)	Receipt of child pornography

The application is based on these facts:
See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

Whitney D. Russell


Applicant's signature

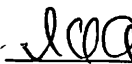
Scott Stein, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 2 Jun 17

City and state: Alexandria VA

 /s/ Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

The property to be searched consists of an Apple iPhone model A1778, serial number DNPSDABEHG7W, and an Apple iPad Model A1674, serial number DMPS66Q8GXQ4, hereinafter the “Devices.” The Devices are currently located at 44965 Aviation Drive, Suite 112, Dulles, VA 20166.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 2252 relating to the distribution, receipt, possession of, and access with intent to view visual depictions of minors engaging in sexually explicit conduct (i.e., child pornography), including:

- a. Visual depictions of minors engaged in sexually explicit conduct;
- b. Information, correspondence, records, documents or other materials (i) constituting evidence of or pertaining to item “a” above; (ii) constituting evidence of or pertaining to the distribution, receipt or possession of item “a” in or affecting interstate or foreign commerce or through any means or facility of interstate and foreign commerce; (iii) constituting evidence of or pertaining to an interest in child pornography or sexual activity with children; and (iv) constituting evidence of identity, knowledge, and intent, including:
 - i. Child erotica;
 - ii. Correspondence, records, or communications, such as voice, video, email, text and chat logs;
 - iii. All records and data associated with the BitTorrent network and any associated software;
 - iv. Diaries, calendars, address books, names, and lists of names and addresses of individuals who may have been contacted through digital mediums and/or the Internet;
 - v. Financial records, including credit card information.
- c. The items listed in “a” and “b” above may be seized in whatever form, visual or aural, and by any means by which they may have been created, stored, or found, including any digital storage device, magnetic storage device, handmade forms, photographic images, film, and video tape (whether developed or undeveloped), books, magazines, printings, typing, facsimiles, and photocopies;
- d. Records or documents evidencing ownership or use of digital media, smart phones, and computer equipment found in the SUBJECT PREMISES, including sales receipts, bills, and handwritten notes.

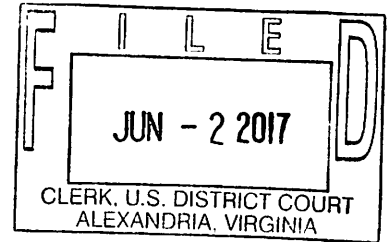
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of any Internet Protocol address to communicate with the BitTorrent file-sharing network, or other child pornography file-sharing sites or websites, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA



IN THE MATTER OF THE SEARCH OF
Apple iPhone model A1778, serial number
DNPSDABEHG7W, and an Apple iPad Model
A1674, serial number DMPS66Q8GXQ4,
CURRENTLY LOCATED AT 44965 Aviation
Drive, Suite 112, Dulles, VA 20166

Case No. 1:17-SW-303

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Scott Stein, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI), have been so employed since 2009, and I am currently assigned to the child exploitation unit. Prior to my employment with HSI, I was employed as a local law enforcement officer with the City of Virginia Beach for approximately six years where I worked as a Detective and as a Master Police Officer. I possess a Master's Degree in Public Administration from Troy University. I have training and experience in the enforcement of the laws of the United States, including the preparation, presentation, and service of subpoenas, affidavits, criminal complaints, search warrants, and arrests warrants.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched consists of an Apple iPhone model A1778, serial number DNPSDABEHG7W, and an Apple iPad Model A1674, serial number DMPS66Q8GXQ4, hereinafter the "Devices." The Devices are currently located at 44965 Aviation Drive, Suite 112, Dulles, VA 20166.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. HSI is currently investigating Jerry Dean Dillingham for receipt of child pornography in violation of Title 18, United States Code, Sections 2252(a)(2). Based on an undercover investigation conducted in June of 2016, a search warrant conducted in August 2016, and a forensic examination of devices recovered pursuant to that search warrant, Dillingham was identified as an individual who was receiving and distributing child pornography using the BitTorrent file-sharing network. The investigation indicated that Dillingham was using Apple devices, among other devices, to receive, distribute, and store child pornography.

7. The Devices are currently in the lawful possession of HSI. On May 31, 2017, acting pursuant to a warrant issued by Magistrate Judge Theresa Carroll Buchanan, HSI agents arrested Dillingham for violations of Title 18, United States Code, Sections 2252(a)(2). During his arrest, Dillingham had the Devices on his person or in his immediate possession. The agents

secured the Devices. Dillingham provided the access passcodes to the devices, thereby relinquishing any reasonable expectation of privacy. Therefore, while the HSI might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

8. The Devices are currently in storage at 44965 Aviation Drive, Suite 112, Dulles, VA 20166. In my training and experience, I know that the Devices have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of HSI.

9. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, internet browser, computer, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and whether the devices were used for illegal activities such as the receipt and distribution of child pornography.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

10. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

11. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

12. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of that use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to receive child pornography, the individual’s electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for

evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

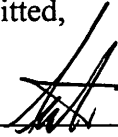
13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

14. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

15. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



SCOTT STEIN
Special Agent
HOMELAND SECURITY
INVESTIGATIONS

Subscribed and sworn to before me
on June 2, 2017:



Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

The property to be searched consists of an Apple iPhone model A1778, serial number DNPSDABEHG7W, and an Apple iPad Model A1674, serial number DMPS66Q8GXQ4, hereinafter the "Devices." The Devices are currently located at 44965 Aviation Drive, Suite 112, Dulles, VA 20166.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 2252 relating to the distribution, receipt, possession of, and access with intent to view visual depictions of minors engaging in sexually explicit conduct (i.e., child pornography), including:

- a. Visual depictions of minors engaged in sexually explicit conduct;
- b. Information, correspondence, records, documents or other materials (i) constituting evidence of or pertaining to item “a” above; (ii) constituting evidence of or pertaining to the distribution, receipt or possession of item “a” in or affecting interstate or foreign commerce or through any means or facility of interstate and foreign commerce; (iii) constituting evidence of or pertaining to an interest in child pornography or sexual activity with children; and (iv) constituting evidence of identity, knowledge, and intent, including:
 - i. Child erotica;
 - ii. Correspondence, records, or communications, such as voice, video, email, text and chat logs;
 - iii. All records and data associated with the BitTorrent network and any associated software;
 - iv. Diaries, calendars, address books, names, and lists of names and addresses of individuals who may have been contacted through digital mediums and/or the Internet;
 - v. Financial records, including credit card information.
- c. The items listed in “a” and “b” above may be seized in whatever form, visual or aural, and by any means by which they may have been created, stored, or found, including any digital storage device, magnetic storage device, handmade forms, photographic images, film, and video tape (whether developed or undeveloped), books, magazines, printings, typing, facsimiles, and photocopies;
- d. Records or documents evidencing ownership or use of digital media, smart phones, and computer equipment found in the SUBJECT PREMISES, including sales receipts, bills, and handwritten notes.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of any Internet Protocol address to communicate with the BitTorrent file-sharing network, or other child pornography file-sharing sites or websites, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.